IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

JASON MYERS and JOHN PARSONS, individually and on behalf of all others similarly situated, Plaintiffs, v. ARTHUR J. GALLAGHER & CO. and GALLAGHER BASSETT SERVICES, INC., Defendants.	)	Case No.: **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT

Plaintiffs Jason Myers and John Parsons ("Plaintiffs") bring this Class Action Complaint against Defendants Arthur J. Gallagher Co. ("Gallagher Co.") and Gallagher Bassett Services, Inc. ("Gallagher Bassett") (collectively "Gallagher" or "Defendants") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. Gallagher is an insurance and insurance brokerage company. Among various types of insurance, Defendants provide insurance brokerage, risk management, human resources, and benefits consulting services.

2. On or about June 30, 2021, Gallagher began notifying customers and state Attorneys General about a data breach that occurred between June 30, 2020 and September 26, 2020 (the "Data Breach").[1] Hackers obtained information from Gallagher including personally identifiable information ("PII") of thousands of its customers, potential customers, employees and

[1] https://oag.ca.gov/system/files/AJG%20-%20Sample%20Notice.pdf (last visited Jul. 23, 2021).

other consumers, including, but not limited to their: names; Social Security numbers; tax identification numbers; driver's license, passport, or other government identification numbers; dates of birth; usernames and passwords; employee identification numbers; financial account information; credit card information; electronic signatures; medical treatment, claim, diagnosis, medication or other medical information; health insurance information; medical record or account numbers; and biometric information.

3. Plaintiffs and Class Members now face a present and imminent lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers and electronic signatures.

4. After the initial notification of Data Breach on June 30, 2021, Gallagher discovered that additional customers and employees were affected and, on or about July 16, 2021, Gallagher began notifying the additional individuals of the Data Breach.

5. After the second notification of Data Breach, Gallagher discovered that even more additional customers and employees were affected and, on or about July 21, 2021, Gallagher began notifying the additional individuals of the Data Breach.

6. As Gallagher well understands given that it provides its business customers with Cyber Liability Insurance, "networks and data are the lifeblood of … business," and "cyber-attacks are increasing in their frequency and their intensity."[2] And it is this exact personal data on its networks that Defendants failed to protect from cyber-attacks.

7. Not only did hackers steal the PII of Plaintiffs and class members, but, upon information and belief, criminals have already used the PII to attempt to steal certain of Plaintiffs' and class members' identities. Hackers accessed and then either used or offered for sale the unencrypted, unredacted, stolen PII to criminals. This stolen PII has great value to hackers. Because of Defendants' Data Breach, customers' PII is still available and may be for sale on the dark web for criminals to access and abuse. Defendants' customers and

[2] https://www.ajg.com/us/insurance/cyber-liability-insurance/ (last visited Jul. 23, 2021).

employees face a current and ongoing lifetime risk of identity theft.

8. As Gallagher acknowledges on its own website: "Due to the prolific nature of cyberattacks, it may be difficult to argue that a prudent expert would not consider and react to cyber risks."[3]

9. The information stolen in cyber-attacks allows the modern thief to assume your identity when carrying out criminal acts such as:

- Using your credit history.
- Making financial transactions on your behalf, including opening credit accounts in your name.
- Impersonating you via mail and/or email.
- Impersonating you in cyber forums and social networks.
- Stealing benefits that belong to you.
- Committing illegal acts which, in turn, incriminate you.

10. Plaintiffs' and Class Members' PII was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and class members. In addition to Defendants' failure to prevent the Data Breach, after discovering the breach, Defendants waited several months to report it to the states' Attorneys General and affected individuals. Defendants have also purposefully maintained secret the specific vulnerabilities and root causes of the breach and have not informed Plaintiffs and class members of that information.

11. As a result of this delayed response, Plaintiffs and class members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their

[3] https://www.ajg.com/us/news-and-insights/2019/11/retirement-plan-cybersecurity/ (last visited Jul. 23, 2021).

respective lifetimes.

12. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect consumers' and employees' PII, (ii) warn its current and former customers, potential customers, and current and former employees of their inadequate information security practices, and (iii) effectively monitor their websites and platforms for security vulnerabilities and incidents (the "Class"). Defendants' conduct amounts to negligence and violates federal and state statutes.

13. Plaintiffs and similarly situated individuals have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished inherent value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) deprivation of rights they possess under California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL"); the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. (the "CCPA"); California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. (the "CLRA"); and Louisiana's Database Security Breach Notification Law, La. Rev. Stat. Ann. §§ 51:3074(A), *et seq.* (the "LDSBNL"); and (v) the continued and certainly an increased risk to their PII, which: (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

PARTIES

14. Plaintiff Jason Myers is a citizen of California, residing in Los Angeles County,

California. Mr. Myers received the Notice of Data Breach from Defendants dated July 21, 2021, on or about that date. The Notice advised that the Data Breach had occurred following a "ransomware event impacting our internal systems," and that Mr. Myers' PII was involved.

15. Plaintiff John Parsons is a citizen of Louisiana, residing in Lincoln Parish, Louisiana. Mr. Parsons received the Notice of Data Breach from Defendants dated July 12, 2021, on or about that date. The Notice advised that the Data Breach had occurred following an "incident that may affect the privacy of some of your information" and that Mr. Parsons' PII was involved. Mr. Parsons was employed by Defendants for approximately three years ending in or about April of 1999.

16. Defendant Arthur J. Gallagher & Co. ("Gallagher Co.") is a Delaware corporation with its principal place of business at 2850 Golf Road, Rolling Meadows, Illinois. Gallagher Co. is one of the largest US-based insurance brokerage, risk management, and HR and benefits consulting firms, providing insurance for alternative risk and captives, casualty, commercial surety bonds insurance, construction bonds, trade credit and political risk, and cyber insurance and has $22.33 billion in assets.[4][5] According to its website, Gallagher Co. employs more than 34,000 people in more than 150 countries and is licensed to sell insurance in all 50 states and the District of Columbia.[6]

17. Gallagher Bassett Services, Inc. ("Gallagher Bassett") is a Delaware corporation with its principal place of business at 2850 Golf Road, Rolling Meadows, Illinois. Gallagher Bassett is a property and casualty third-party administrator.[7] According to its website, Gallagher Bassett employs more than 4,700 people at over 110 branch locations providing its services to over 3,500 clients.[8]

---

[4] https://www.ajg.com/us/about-us/ (last visited Jul. 23, 2021).

[5] https://www.marketwatch.com/investing/stock/ajg/financials/balance-sheet (last visited Jul. 23, 2021).

[6] https://www.ajg.com/us/about-us/ (last visited Jul. 23, 2021).

[7] https://www.ajg.com/us/insurance/claims/claims-management-third-party-administration/ (last visited Jul. 27, 2021).

[8] *Id*.

JURISDICTION AND VENUE

18. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendants.

19. This Court has personal jurisdiction over Defendants because Defendants' principal places of business are located within this District.

20. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendants reside within this judicial district and a substantial part of the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

21. Gallagher is one of the largest U.S.-based insurance brokerage, risk management, and HR and benefits consulting firms, providing insurance for alternative risk and captives, casualty, commercial surety bonds insurance, construction bonds, trade credit and political risk, and cyber insurance and has $22.33 billion in assets.[9] According to their website, Gallagher employs more than 34,000 people in more than 150 countries, and is licensed to sell insurance in all 50 states and the District of Columbia.[10]

22. In the ordinary course of doing business with Defendants, employees, customers and prospective customers are required to provide Defendants with sensitive PII such as:

a. Full names;

b. Social Security numbers;

---

[9] https://www.ajg.com/us/about-us/ (last visited Jul. 23, 2021); https://www.marketwatch.com/investing/stock/ajg/financials/balance-sheet (last visited Jul. 23, 2021).

[10] https://www.ajg.com/us/about-us/ (last visited Jul. 23, 2021).

c. tax identification numbers;

d. driver's license numbers;

e. passport numbers;

f. government identification numbers;

g. dates of birth;

h. employee identification numbers;

i. financial account information;

j. credit card information;

k. electronic signatures;

l. medical treatment, claim, diagnosis, or other medical information;

m. medical record numbers;

n. patient account numbers; and

o. biometric information.

23. In addition to the types of information Defendants collect from employees and consumers listed above, Defendants collect personal information through other insurers, consumer reporting agencies, their affiliated companies, and other third parties and track and maintain record of internet usage information and inferences from PII collected.[11] This personal information includes personal details, contact details, bank details (including account numbers and financial information from consumer-reporting agencies), and policy details.[12]

24. In the course of collecting PII from employees and consumers, including Plaintiffs, Defendants promise to provide confidentiality and security for personal information, including by promulgating and placing privacy policies on their website.

25. Defendants promise that they will protect their employees and customers' privacy and remain in compliance with statutory privacy requirements. For example, Defendants state on their website:

---

11 https://www.ajg.com/us/privacy-policy/ (last visited Jul. 23, 2021).

12 *Id*.

> We implement technical, organizational, administrative and physical measures to help ensure a level of security appropriate to the risk to the personal information we collect, use, disclose and process. These measures are aimed at ensuring the on-going integrity and confidentiality of personal information.[13]

26. Defendants also represent on their website: "We restrict access to your personal information to those who require access to such information for legitimate, relevant business purposes."[14] The types of information Gallagher collects from its customers include personal details (e.g., name, date of birth); contact details (e.g., phone number, email address, postal address or mobile number); government issued identification details (e.g., social security and national insurance numbers, passport details); health and medical details (e.g., health certificates); policy details (e.g., policy numbers and types); bank details (e.g., payment details, account numbers and sort codes); driving license details; online log-in information (e.g., username, password, answers to security questions); information relating to any claims; occupation information, and other information and inferences from PII collected.[15]

The Data Breach

27. On or about September 26, 2020, Gallagher detected an apparent ransomware attack on its internal network.

28. Gallagher began to investigate the situation by taking its global systems offline and it launched an investigation with the assistance of a third-party.

29. Gallagher informed certain media outlets of the ransomware attack as early as September 29, 2020.[16]

30. On May 24, 2021, Gallagher concluded that certain information was taken from Gallagher's internal network by an unauthorized party.

31. A full year after the attack took place, Gallagher reported to the California Attorney General's office that between June 3, 2020 and September 26, 2020 an unauthorized party gained

---

13 *Id*.
14 *Id*.
15 *Id*.
16 https://securityaffairs.co/wordpress/108925/malware/ajg-ransomware-attack.html (last visited Jul. 26, 2021).

access to Gallagher's internal network and accessed certain individuals' information.

32. According to the Notices of Data Breach letters and letters sent to state Attorneys General, Gallagher "detected a ransomware event impacting [its] internal systems" and "determined that an unknown party accessed or acquired data contained within certain segments of [its] network between June 3, 2020 and September 26, 2020."[17]

33. According to the Notices, Gallagher "took [its] systems offline as a precautionary measure, initiated response protocols, launched an investigation with the assistance of third-party cybersecurity and forensic specialists, implemented our business continuity plans to minimize disruption to our customers, and ensured the ongoing security of [its] systems." Gallagher's investigation concluded on May 24, 2021.[18]

34. However, despite first learning of the Data Breach in September 2020 and concluding the investigation in May 2021, Defendants did not take any "measures" to notify affected Class Members until on or about June 30, 2021.

35. Additionally, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again has not been shared with regulators or Plaintiffs and Class members, who retain a vested interest in ensuring that their information remains protected.

36. While Defendants did not bother to take any "measures" to notify affected Class members until more than a year after the Data Breach, they did announce the "ransomware" attack as early as September 2020.[19]

37. Any Class member who saw the September 2020 media reports on the subject but

---

[17] https://oag.ca.gov/system/files/AJG%20-%20Sample%20Notice.pdf (last visited Jul. 23, 2021).

[18] *Id*.

[19] https://securityaffairs.co/wordpress/108925/malware/ajg-ransomware-attack.html (last visited Jul. 26, 2021).

who did not receive any Notice of Data Breach likely concluded that their data was not impacted in the Data Breach and therefore would not have known of the need to take action to protect themselves.

38. The Notices offered "access, at no cost, to identity and credit monitoring services for twenty-four months through Kroll." The Notices advised the recipients to "remain vigilant against incidents of identity theft and fraud."[20]

Defendants Were Aware of the Risks of a Data Breach

39. Defendants had obligations created by contract, industry standards, common law, and representations made to Plaintiffs and Class members, to keep their PII confidential and to protect it from unauthorized access and disclosure.

40. Plaintiffs and Class members provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

41. Defendants' data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches in the banking/credit/financial services industry preceding the date of the breach.

42. Data breaches, including those perpetrated against the banking/credit/financial sector of the economy, have become widespread. In fact, over 62% of the 164 million sensitive records exposed in data breaches in 2019 were exposed in breaches involving the banking/credit/financial sector. [21]

43. Indeed, data breaches, such as the one experienced by Defendants, have become so

---

[20] *Id.*

[21] https://www.idtheftcenter.org/wp-content/uploads/2020/01/01.28.2020_ITRC_2019-End-of-Ye ar-Data-Breach-Report_FINAL_Highres-Appendix.pdf (last visited Dec. 10, 2020).

notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public and to anyone in Defendants' industry, including Defendants.

44. According to the Federal Trade Commission ("FTC"), identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[22] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[23]

45. The PII of Plaintiffs and members of the Classes was taken by hackers to engage in identity theft or and or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

46. Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and members of the Class, including Social Security numbers, driver's license or state identification numbers, and/or dates of birth, and of the foreseeable consequences that would occur if Defendants' data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and members of the Class a result of a breach.

47. Plaintiffs and members of the Class now face years of constant surveillance of their

---

[22] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf (last visited Apr. 7, 2021).

[23] *Id*. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id*.

financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

48. The injuries to Plaintiffs and members of the Class were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiffs and members of the Class.

Defendants Failed to Comply with FTC Guidelines

49. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

50. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their networks' vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

51. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

52. The FTC has brought enforcement actions against businesses for failing to protect consumer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. Defendants failed to properly implement basic data security practices, and their failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

54. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those

with a need for administrator accounts should only use them when necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[24]

55. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks….

- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different

[24] https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last visited Jul. 27, 2021).

domain (e.g., .com instead of .net) . . . .

- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it . . . .

- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.

- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic . . . .[25]

56. Defendants were at all times fully aware of their obligation to protect the PII of customers, prospective customers and employees. Defendants were also aware of the significant repercussions that would result from their failure to do so.

Defendants Failed to Comply with Industry Standards

57. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendants' cybersecurity practices.

58. Best cybersecurity practices that are standard in the financial services industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such

[25] https://us-cert.cisa.gov/ncas/tips/ST19-001 (last visited Jul. 27, 2021).

as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.

59. Upon information and belief, Defendants failed to meet the minimum standards of the following cybersecurity frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are established standards in reasonable cybersecurity readiness.

60. These foregoing frameworks are existing and applicable industry standards in Defendants' industry, and Defendants failed to comply with these accepted standards, thereby opening the door to the cyber-attack and causing the Data Breach.

61. Given that Defendants were storing the PII of tens of thousands of current and former employees and their beneficiaries and dependents, as well as millions of customers, collected since at least 1999, Defendants could and should have implemented all of the above measures to prevent and detect ransomware attacks.

62. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of hundreds of thousands of current and former employees and customers, including Plaintiffs and Class Members.

The Value of PII to Cyber Criminals

63. Businesses that store personal information are likely to be targeted by cyber criminals. Credit card and bank account numbers are tempting targets for hackers. However, information such as dates of birth and Social Security numbers are even more attractive to hackers;

they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

64. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[26]

65. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration ("SSA") stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[27]

66. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

67. Even then, a new Social Security number may not be effective. According to Julie

---

[26] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs (last visited Apr. 7, 2021).

[27] SSA, *Identity Theft and Your Social Security Number*, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 7, 2021).

Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[28]

68. Furthermore, as the SSA warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[29]

69. Here, the unauthorized access left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. The personal data of Plaintiffs and members of the Class stolen in the Data Breach constitutes a dream for hackers and a nightmare for Plaintiffs and the Class. Stolen personal data of Plaintiffs and members of the Classes represents essentially one-stop shopping for identity thieves.

70. The FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

---

[28] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Apr. 7, 2021).

[29] SSA, *Identity Theft and Your Social Security Number*, SSA Publication No. 05-10064 (Jun. 2018), http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Apr. 7, 2021).

71. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for years. According to the United States Government Accountability Office ("GAO") Report to Congressional Requesters:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[30]

72. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. The stolen personal data of Plaintiffs and members of the Class has a high value on both legitimate and black markets.

73. Identity thieves may commit various types of crimes such as immigration fraud, obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

74. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns. Defendants' former and current customers and employees whose Social Security numbers have been compromised now face a real, present, imminent and substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

75. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data

---

[30] *See* https://www.gao.gov/assets/gao-07-737.pdf (June 2007) at 29 (last visited Apr. 7, 2021).

breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change — Social Security number, driver's license number or government-issued identification number, name, and date of birth.

76. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[31]

77. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police. An individual may not know that his or her driver's license was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud, or until the individual attempts to lawfully apply for unemployment and is denied benefits (due to the prior, fraudulent application and award of benefits).

Plaintiffs' and Class Members' Damages

78. To date, Defendants have done absolutely nothing to provide Plaintiffs and Class members with relief for the damages they have suffered as a result of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendants have only offered twenty-four months of identity monitoring services, and it is unclear whether that credit monitoring was only offered to certain affected individuals (based upon the type of data stolen), or to all persons whose data was compromised in the Data Breach.

79. Moreover, the twenty-four months of credit monitoring offered to persons whose PII was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity

[31] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Apr. 7, 2021).

theft and financial fraud.

80. Defendants entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class members' PII.

81. Plaintiffs and Class members have been damaged by the compromise of their PII in the Data Breach.

82. Plaintiffs and Class members presently face substantial risk of out-of-pocket fraud losses such as loans opened in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

83. Plaintiffs and Class members have been, and currently face substantial risk of being targeted now and in the future, subjected to phishing, data intrusion, and other illegal based on their PII as potential fraudsters could use that information to target such schemes more effectively to Plaintiffs and Class members.

84. Plaintiffs and Class members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

85. Plaintiffs and Class members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in data breach cases.

86. Plaintiffs and Class members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

87. Plaintiffs and Class members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach

88. Moreover, Plaintiffs and Class members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure

that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password protected.

89. Further, as a result of Defendants' conduct, Plaintiffs and Class members are forced to live with the anxiety that their PII —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

90. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

The Plaintiffs' Experiences

Plaintiff John Parsons

91. Plaintiff John Parsons worked for Gallagher from approximately 1996 until April of 1999. Mr. Parsons was required by Gallagher to supply it with his PII, including but not limited to his full name, then-current mailing address, and Social Security number.

92. Mr. Parsons received the Notice of Data Breach from Defendants, dated July 12, 2021, on or about that date. The Notice stated that the exposed PII included Mr. Parsons' name and Social Security number.

93. As a result of receiving the Data Breach notice, Mr. Parsons has spent time dealing with the consequences of the breach, including confirming the legitimacy of the Data Breach, reviewing the information compromised by the breach, self-monitoring his accounts, exploring credit monitoring and identity theft insurance options, and exploring the free credit monitoring service offered by Defendants.

94. Mr. Parsons is not aware of any other data breaches that could have resulted in the theft of his Social Security number. He is very careful about sharing his PII, and has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

95. Mr. Parsons stores any and all documents containing his PII in a safe and secure digital location and destroys any documents he receives in the mail that contain any of his PII or

that may contain any information that could otherwise be used to compromise his Social Security number.

96. Mr. Parsons suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Parsons entrusted to Defendants for the purpose of his employment by Defendants and which was compromised in and as a result of the Data Breach.

97. Mr. Parsons also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of his privacy.

98. Mr. Parsons has suffered imminent and impending injury arising from the present and substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

99. Mr. Parsons has become worried about this theft of his PII and has a continuing interest in ensuring that Defendants protect and safeguard his PII, which remains in their possession, from future breaches.

Plaintiff Jason Myers

100. Plaintiff Jason Myers received the Notice of Data Breach from Gallagher, dated July 21, 2021, on or about that date. The Notice stated that the exposed PII included Mr. Myers' name and medical claim information.

101. As a result of receiving the Data Breach notice, Mr. Myers has spent time dealing with the consequences of the breach, including confirming the legitimacy of the Data Breach, reviewing the account compromised by the breach, self-monitoring his accounts, exploring credit monitoring and identity theft insurance options, and signing up for the free credit monitoring service offered by Defendants.

102. Mr. Myers has experienced a dramatic increase in the number of spam telephone calls he receives following the Data Breach.

103. Mr. Myers is not aware of any other data breaches that could have resulted in the theft of his PII. He is very careful about sharing his PII, and has never knowingly transmitted

unencrypted PII over the internet or any other unsecured source.

104. Mr. Myers stores any and all documents containing his PII in a safe and secure digital location and destroys any documents he receives in the mail that contain any of his PII or that may contain any information that could otherwise be used to compromise his payment card accounts.

105. Mr. Myers suffered actual injury in being forced to review spam telephone calls and in paying money to, or purchasing products from, Defendants or third-parties who used Defendants' services during the Data Breach—expenditures which he would not have made had Defendants disclosed that they lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

106. Mr. Myers suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he entrusted to Defendants for the purpose of purchasing Defendants' products and which was compromised in and as a result of the Data Breach.

107. Mr. Myers also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has serious concerns for the loss of his privacy.

108. Mr. Myers has suffered imminent and impending injury arising from the present and substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of criminals.

109. Mr. Myers has become worried about this theft of his PII and has a continuing interest in ensuring that Defendants protect and safeguard his PII, which remains in their possession, from future breaches.

CLASS ALLEGATIONS

110. Plaintiffs bring this nationwide class action pursuant to rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following classes:

> All natural persons residing in the United States whose PII was

compromised in the Data Breach announced by Defendants on or about June 30, 2021 (the "Nationwide Class").

111. The California Subclass is defined as follows:

All natural persons residing in California whose PII was compromised in the Data Breach announced by Defendants on or about June 30, 2021 (the "California Subclass").

112. The Louisiana Subclass is defined as follows:

All natural persons residing in Louisiana whose PII was compromised in the Data Breach announced by Defendants on or about June 30, 2021 (the "Louisiana Subclass").

113. The California and Louisiana Subclasses are collectively referred to herein as the "Statewide Subclasses," and, together with the Nationwide Class, are collectively referred to herein as the "Classes" or the "Class."

114. Excluded from the Classes are all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out, and all judges assigned to hear any aspect of this litigation and their immediate family members.

115. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

116. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendant has indicated that the PII of hundreds of thousands of individuals has been improperly accessed in the Data Breach, and the Classes are apparently identifiable within Defendants' records.

117. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual members of the Classes. These include:

a. When Defendants actually learned of the Data Breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Classes to exercise due care in collecting,

storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing the PII of Plaintiffs and members of the Classes;

e. Whether Defendants acted negligently in connection with the monitoring and/or protection of PII belonging to Plaintiffs and members of the Classes;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep the PII of Plaintiffs and members of the Classes secure and to prevent loss or misuse of that PII;

g. Whether Defendants have adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

h. Whether Defendants caused Plaintiffs' and members of the Classes damage;

i. Whether Defendants violated the law by failing to promptly notify Plaintiffs and members of the Classes that their PII had been compromised;

j. Whether Plaintiffs and the other members of the Classes are entitled to credit monitoring and other monetary relief;

k. Whether Defendants violated California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL");

l. Whether Defendants violated the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. (the "CCPA");

m. Whether Defendants violated California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. (the "CLRA"); and

n. Whether Defendants violated Louisiana's Database Security Breach Notification Law, La. Rev. Stat. Ann. § 51:3074(A), *et seq.* (the "LDSBNL");

118. **Typicality**: Plaintiffs' claims are typical of those of the other members of the Classes because all had their PII compromised as a result of the Data Breach due to Defendants'

misfeasance.

119. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the members of the Classes. Plaintiffs' counsel are competent and experienced in litigating privacy-related class actions.

120. **Superiority and Manageability**: Under rule 23(b)(3) of the Federal Rules of Civil Procedure, a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual member of the Classes are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

121. Class certification is also appropriate under Rule 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Classes, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Nationwide Class as a whole and as to each of the Statewide Subclasses as a whole.

122. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiffs and the members of the Classes to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security

procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

e. Whether members of the Classes are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses Against All Defendants)

123. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 122.

124. Defendants owed a duty to Plaintiffs and the members of the Classes to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

125. The legal duties owed by Defendants to Plaintiffs and the members of the Classes include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and members of the Classes in their possession;

b. To protect PII of Plaintiffs and members of the Classes in their possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and members of the Classes of the Data Breach.

126. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45(a) (the "FTC Act"), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the

Federal Trade Commission, the unfair practices by companies such as Defendants of failing to use reasonable measures to protect PII.

127. Various FTC publications and data security breach orders further form the basis of Defendants' duty. Plaintiffs and members of the Classes are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and by not complying with industry standards.

128. Defendants breached their duties to Plaintiffs and members of the Classes. Defendants knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the fact that data breaches have been surging since 2016.

129. Defendants knew or should have known that their security practices did not adequately safeguard the PII of Plaintiffs and the other members of the Classes.

130. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the PII of Plaintiffs and the Classes from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and other members of the Classes during the period it was within Defendants' possession and control.

131. Defendants breached the duties they owe to Plaintiffs and members of the Classes in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect employees' and customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the Data Breach;

c. Failing to act despite knowing or having reason to know that their systems were vulnerable to attack; and

d. Failing to timely and accurately disclose to customers and employees that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

132. Due to Defendants' conduct, Plaintiffs and members of the Classes are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used for identity theft and other types of financial fraud against the members of the Classes.

133. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

134. As a result of Defendants' negligence, Plaintiffs and members of the Classes suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession and subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiffs and members of the Classes, including ongoing credit monitoring.

135. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiffs and the other members of the Classes suffered was the direct and proximate result of Defendants' negligent conduct.

/ / /

/ / /

/ / /

SECOND CLAIM FOR RELIEF
Negligence *Per Se*
(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses Against All Defendants)

136. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 122.

137. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

138. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendants' magnitude, including, specifically, the immense damages that would result to Plaintiffs and members of the Classes due to the valuable nature of the PII at issue in this case—including Social Security numbers.

139. Defendants' violations of Section 5 of the FTC Act constitute negligence *per se*.

140. Plaintiffs and members of the Classes are within the class of persons that the FTC Act was intended to protect.

141. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Classes.

142. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and members of the Classes have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,

detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and members of the Classes.

143. Additionally, as a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and members of the Classes have suffered and will suffer the continued risks of exposure of their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession.

THIRD CLAIM FOR RELIEF
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*—Unlawful Business Practices
(On Behalf of Plaintiff Jason Myers and the Nationwide Class or, in the Alternative, the California Subclass Against All Defendants)

144. Plaintiff Jason Myers re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 122.

145. Defendants have violated Cal. Bus. and Prof. Code § 17200, *et seq.*, by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the services provided to the Nationwide Class or, in the alternative, the California Subclass.

146. Defendants engaged in unlawful acts and practices with respect to their services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and Nationwide Class and California Subclass members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and the Nationwide Class and California Subclass members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiffs and the Nationwide Class and California Subclass members. Defendants also violated: the California Consumer Privacy Act, Cal. Civ. Code § 1798.100, *et seq*. and the California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*., as alleged below; and also the California Financial Information Privacy Act, California Financial Code § 4052.5; the Graham Leach Bliley Act Privacy Rule, 16 C.F.R. Part 313, and Reg. P, 12 C.F.R. Part 1016; and Article 1, § 1 of the California Constitution.

147. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the data breach to Nationwide and California Subclass members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendants still have not provided such information to Plaintiffs and the Nationwide Class and California Subclass members.

148. As a direct and proximate result of Defendants' unlawful practices and acts, Plaintiffs and the Nationwide Class and California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Nationwide Class and California Subclass members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

149. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Nationwide Class and California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in

engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide Class and California Subclass.

150. Nationwide Class and California Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiffs and Nationwide Class and California Subclass members of money or property that Defendants may have acquired by means of their unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unlawful and unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

FOURTH CLAIM FOR RELIEF
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq*.—Unfair Business Practices
(On Behalf of Jason Myers and the Nationwide Class or, in the Alternative, the California Subclass Against All Defendants)

151. Plaintiff Jason Myers re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 122.

152. Defendants engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and the Nationwide Class and California Subclass members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Nationwide Class and California Subclass members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Nationwide Class and California Subclass members. They were likely to deceive the public into believing their PII was securely stored when it was not. The harm these practices caused to Plaintiffs and the Nationwide Class and California Subclass members outweighed their utility, if any.

153. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and

security measures and protect Nationwide Class and California Subclass members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiffs and Nationwide Class and California Subclass members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiffs and the Nationwide Class and California Subclass members outweighed their utility, if any.

154. As a direct and proximate result of Defendants' acts of unfair practices, Plaintiffs and the Nationwide Class and California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of Nationwide Class and California Subclass members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

155. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard the Nationwide Class and California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the Nationwide Class and California Subclasses.

156. Nationwide Class and California Subclass members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and the Nationwide Class and California Subclass members of money or property that the Defendants may have acquired by means of their unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of their unfair business practices, declaratory relief, attorneys' fees and costs, and injunctive or other equitable relief.

/ / /

/ / /

FIFTH CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq*.
(On Behalf of Plaintiff Jason Myers and the
California Subclass Against All Defendants)

157. Plaintiff Jason Myers re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 122.

158. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff Myers' and California Subclass members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff Myers and California Subclass members.

159. As a direct and proximate result of Defendants' acts, Plaintiff Myers' and the California Subclass members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure through Gallagher's computer systems and/or from the dark web, where hackers further disclosed Gallagher's customers', employees', former employees' and their dependents' PII.

160. As a direct and proximate result of Defendants' acts, Plaintiff Myers and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of California Subclass members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

161. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff Myers and the California Subclass members.

162. Defendant Gallagher Co. is a public company that is organized or operated for the profit or financial benefit of its shareholders, with over $22 billion in assets. Gallagher Co. and

Gallagher Co.'s wholly-owned subsidiary, Gallagher Bassett, collect consumers' PII as defined in Cal. Civ. Code § 1798.140.

163. At this time, Plaintiff Myers and California Subclass members seek only actual pecuniary damages suffered as a result of Defendants' violations of the CCPA, injunctive and declaratory relief, attorneys' fees and costs, and any other relief the court deems proper.

164. Concurrently with the filing of this complaint, Plaintiff Myers provided written notice to Defendants identifying the specific provisions of this title he alleges they have violated. Assuming Defendants do not cure the Data Breach within 30 days, and Plaintiff Myers believes any such cure is not possible under these facts and circumstances, Plaintiff Myers intends to amend this complaint to also seek the greater of statutory damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater. *See* Cal. Civ. Code § 1798.150(b).

SIXTH CLAIM FOR RELIEF
Violation of California's Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*.
(On Behalf of Plaintiff Jason Myers and the California Subclass Against All Defendants)

165. Plaintiff Jason Myers re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 122.

166. The California Consumers Legal Remedies Act, Cal. Civ. Code § 1750, *et seq*. ("CLRA"), was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers. Defendants' acts, omissions, representations and practices as described herein fall within the CLRA because the design, development, and marketing of Defendants' insurance services are intended to and did result in sales of insurance services.

167. Plaintiff Jason Myers and the other California Subclass members are consumers within the meaning of Cal. Civ. Code §1761(d).

168. Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers. By omitting key information about the safety and security of the Network

and deceptively representing that they adequately maintained such information, Defendants violated the CLRA. Defendants had exclusive knowledge of undisclosed material facts, namely, that their network was defective and/or unsecure, and withheld that knowledge from California Subclass members.

169. Defendants' acts, omissions, misrepresentations, and practices alleged herein violated the following provisions of section 1770 the CLRA, which provides, in relevant part, that:

> (a) The following unfair methods of competition and unfair or deceptive acts or practices undertaken by any person in a transaction intended to result or which results in the sale or lease of goods or services to any consumer are unlawful:
>
> (5) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have . . . .
>
> (7) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another.
>
> (9) Advertising goods or services with intent not to sell them as advertised.
>
> (14) Representing that a transaction confers or involves rights, remedies, or obligations which it does not have or involve, or which are prohibited by law.
>
> (16) Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

For purposes of the CLRA, omissions are actionable along with representations.

170. Defendants stored California Subclass members' PII on their network. Defendants represented to California Subclass members that their network was secure and that their PII would remain private. Gallagher engaged in deceptive acts and business practices by providing in its Privacy Policy: "We implement technical, organizational, administrative and physical measures to help ensure a level of security appropriate to the risk to the personal information we collect, use, disclose and process;" and "[w]e restrict access to your personal information to those who require access to such information for legitimate, relevant business purposes."[32]

---

[32] https://www.ajg.com/us/privacy-policy/ (last visited Jul. 27, 2021).

171. Defendants knew or should have known that they did not employ reasonable measures that would have kept California Subclass members' PII secure and prevented the loss or misuse of their PII. For example, Defendants failed to take reasonable steps to prevent the loss of PII through their servers through appropriate encryption and industry best practices.

172. Defendants' deceptive acts and business practices induced California Subclass members to provide PII, including Social Security numbers and driver's license numbers, for the purchase of insurance services. But for these deceptive acts and business practices, California Subclass members would not have purchased insurance services, or would not have paid the prices they paid for the insurance services.

173. Defendants' representations that they would secure and protect California Subclass members' PII in their possession were facts that reasonable persons could be expected to rely upon when deciding whether to purchase insurance services.

174. California Subclass members were harmed as the result of Defendants' violations of the CLRA, because their PII was compromised, placing them at a greater risk of identity theft; they lost the unencumbered use of their PII; and their PII was disclosed to third parties without their consent.

175. California Subclass members suffered injury in fact and lost money or property as the result of Defendants' failure to secure their PII; the value of their PII was diminished as the result of Defendants' failure to secure their PII; and they have expended time and money to rectify or guard against further misuse of their PII.

176. Defendants' conduct alleged herein was oppressive, fraudulent, and/or malicious, thereby justifying an award of punitive damages.

177. As the result of Defendants' violations of the CLRA, Plaintiff Myers, on behalf of himself, California Subclass members, and the general public of the State of California, seeks injunctive relief prohibiting Defendants from continuing these unlawful practices pursuant to California Civil Code § 1782(a)(2), and such other equitable relief, including restitution, and a declaration that Defendants' conduct violated the CLRA.

178. Pursuant to Cal. Civ. Code § 1782, concurrently with the filing of this complaint, Plaintiff Myers mailed Defendants notice in writing, via U.S. certified mail, of their particular violations of Cal. Civ. Code § 1770 of the CLRA and demanded that they rectify the actions described above by providing complete monetary relief, agreeing to be bound by Defendants' legal obligations, and to give notice to all affected customers of their intent to do so. If Defendants fail to respond to the letter within 30 days and to take the actions demanded to rectify their violations of the CLRA, Plaintiff Myers will amend this complaint to seek damages and attorneys' fees as allowed by the CLRA.

SEVENTH CLAIM FOR RELIEF
Violation of the Louisiana Database Security Breach Notification Law, La. Rev. Stat. Ann. § 51:3074(A), *et seq*.
(On Behalf of Plaintiff John Parsons and the Louisiana Subclass Against All Defendants)

179. Plaintiff John Parsons re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 122.

180. Gallagher is a business that owns or licenses computerized data that includes personal information as defined by La. Rev. Stat. Ann. § 51:3073(4)(a).

181. Plaintiff Parsons' and Louisiana Subclass members' PII includes personal information as defined by La. Rev. Stat. Ann. § 51:3073(4)(a) and as covered by La. Rev. Stat. Ann. § 51:3074(C).

182. Gallagher is required to accurately notify Plaintiff Parsons and Louisiana Subclass members if it becomes aware of a breach of its data security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff Parsons' and Louisiana Subclass members' personal information in the most expedient time possible and without unreasonable delay under La. Rev. Stat. Ann. § 51:3074(D).

183. Because Gallagher was aware of a breach of its security system that was reasonably likely to have caused unauthorized persons to acquire Plaintiff Parsons' and Louisiana Subclass

members' personal information, Gallagher had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by La. Rev. Stat. Ann. § 51:3074(D).

184. By failing to disclose the Data Breach in a timely and accurate manner, Gallagher violated La. Rev. Stat. Ann. § 51:3074(D).

185. As a direct and proximate result of Gallagher's violations of La. Rev. Stat. Ann. § 51:3074(D), Plaintiff and Louisiana Subclass members suffered damages, as described above.

186. Plaintiff John Parsons and Louisiana Subclass members seek all monetary and non-monetary relief allowed by law under La. Rev. Stat. Ann. § 51:3075, including actual damages and any other relief that is just and proper.

EIGHTH CLAIM FOR RELIEF
Breach of Implied Contract
(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses Against All Defendants)

187. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 122.

188. When Plaintiffs and Nationwide Class members provided their PII to Defendants in exchange for Defendants' products, they entered into implied contracts with Defendants under which—and by mutual assent of the parties—Defendants agreed to take reasonable steps to protect their PII.

189. Defendants solicited and invited Plaintiffs and Nationwide Class members to provide their PII as part of Defendants' regular business practices and as essential to the sales and employment transactions entered into between Defendants on the one hand and Plaintiffs and Nationwide Class members on the other. This conduct thus created implied contracts between Plaintiffs and Nationwide Class members on the one hand, and Defendants on the other hand. Plaintiffs and Nationwide Class members accepted Defendants' offers by providing their PII to Defendants in connection with their purchases from and employment with Defendants.

190. When entering into these implied contracts, Plaintiffs and Nationwide Class members reasonably believed and expected that Defendants' data security practices complied with relevant laws, regulations, and industry standards.

191. Defendants' implied promise to safeguard Plaintiffs' and Nationwide Class members' PII is evidenced by a duty to protect and safeguard PII that Defendants required Plaintiffs and Nationwide Class members to provide as a condition of entering into consumer transactions and employment relationships with Defendants.

192. Plaintiffs and Nationwide Class members paid money to Defendants to purchase products or services from Defendants or they provided services to Defendants as employees. Plaintiffs and Nationwide Class Members reasonably believed and expected that Defendants would use part of funds received as a result of the purchases or services provided to obtain adequate data security. Defendants failed to do so.

193. Plaintiffs and Nationwide Class members, on the one hand, and Defendants, on the other hand, mutually intended—as inferred from customers' continued use of Defendants' insurance services and/or continued employment by Defendants—that Defendants would adequately safeguard PII. Defendants failed to honor the parties' understanding of these contracts, causing injury to Plaintiffs and Nationwide Class members.

194. Plaintiffs and Nationwide Class members value data security and would not have provided their PII to Defendants in the absence of Defendants' implied promise to keep the PII reasonably secure.

195. Plaintiffs and Nationwide Class embers fully performed their obligations under their implied contracts with Defendants.

196. Defendants breached their implied contracts with Plaintiffs and Nationwide Class members by failing to implement reasonable data security measures and permitting the Data Breach to occur.

197. As a direct and proximate result of Defendants' breaches of the implied contracts, Plaintiffs and Nationwide Class members sustained damages as alleged herein.

198. Plaintiffs and Nationwide Class members are entitled to compensatory, consequential, and other damages suffered as a result of the Data Breach.

199. Plaintiffs and Nationwide Class members also are entitled to injunctive relief requiring Defendants to, *inter alia*, strengthen their data security systems and monitoring procedures, conduct periodic audits of those systems, and provide credit monitoring and identity theft insurance to Plaintiffs and Nationwide Class members.

NINTH CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses Against All Defendants)

200. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 122.

201. Defendants owe duties of care to Plaintiffs and Nationwide Class members which require them to adequately secure their PII.

202. Defendants still possess Plaintiffs' and Nationwide Class members' PII.

203. Defendants do not specify in either of the two *Notice of Data Breach* letters what steps they have taken to prevent a data breach from occurring again.

204. Plaintiffs and Nationwide Class members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

205. Plaintiffs, therefore, seek a declaration that (1) each of Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to

promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and security checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Nationwide Class members for a period of ten years; and

h. Meaningfully educating Plaintiffs and Nationwide Class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

TENTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiffs, the Nationwide Class, and the Statewide Subclasses Against All Defendants)

206. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 122.

207. Defendants benefited from receiving Plaintiffs' and Nationwide Class members' PII by their ability to retain and use that information for their own benefit. Defendants understood this benefit.

208. Defendants also understood and appreciated that Plaintiffs' and Nationwide Class members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

209. Plaintiffs and Nationwide Class members who were customers of Defendants conferred a monetary benefit upon Defendants in the form of monies paid for services from Defendants.

210. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Nationwide Class members. Defendants also benefited from the receipt of Plaintiffs' and Nationwide Class members' PII, as Defendants used it to facilitate the transfer of information and payments between the parties.

211. The monies that Plaintiffs and Nationwide Class members paid to Defendants for services were to be used by Defendants, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

212. Defendants also understood and appreciated that Plaintiffs' and Nationwide Class members' PII was private and confidential, and its value depended upon Defendants maintaining the privacy and confidentiality of that PII.

213. But for Defendants' willingness and commitment to maintain privacy and confidentiality, that PII would not have been transferred to and untrusted with Defendants. Indeed, if Defendants had informed Plaintiffs and Nationwide Class members that their data and cyber security measures were inadequate, Defendants would not have been permitted to continue to operate in that fashion by regulators, its shareholders, and its consumers.

214. As a result of Defendants' wrongful conduct, Defendants have been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and Nationwide Class members. Defendants continue to benefit and profit from their retention and use of the PII while its value to Plaintiffs and Nationwide Class Members has been diminished.

215. Defendants' unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged in this complaint, including compiling, using, and retaining Plaintiffs'

and Nationwide Class Members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

216. As a result of Defendants' conduct, Plaintiffs and Nationwide Class members suffered actual damages in an amount equal to the difference in value between the amount Plaintiffs and Nationwide Class members paid for their purchases with reasonable data privacy and security practices and procedures and the purchases they actually received with unreasonable data privacy and security practices and procedures.

217. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Nationwide Class members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Nationwide Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

218. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Nationwide Class members all unlawful or inequitable proceeds they received as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Nationwide Class members and Statewide Subclass members, request judgment against Defendants and that the Court grant the following:

A. An order certifying the Classes as defined herein, and appointing Plaintiffs and their counsel to represent the Classes;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of the PII belonging to Plaintiffs and the members of the Classes;

C. An order requiring Defendants to:

a. Engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration

tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engage third-party security auditors and internal personnel to run automated security monitoring;

c. Audit, test, and train their security personnel regarding any new or modified procedures;

d. Segment their user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conduct regular database scanning and security checks;

f. Routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchase credit monitoring services for Plaintiffs and Nationwide Class members for a period of ten years; and

h. Meaningfully educate Plaintiffs and Nationwide Class members about the threats they face as a result of the loss of their PII to third parties, as well as the steps they must take to protect themselves.

D. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiffs and all members of the Classes;

E. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

F. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

G. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: July 29, 2021

Respectfully Submitted,

WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC

By: */s/ Carl V. Malmstrom*
CARL V. MALMSTROM
111 W. Jackson Blvd., Suite 1700
Chicago, IL 60604
Telephone: (312) 984-0000
Facsimile: (212) 545-4653
malmstrom@whafh.com

RACHELE R. BYRD
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLP
750 B Street, Suite 1820
San Diego, CA 92101
Telephone: (619) 239-4599
Facsimile: (619) 234-4599
byrd@whafh.com

M. ANDERSON BERRY
GREGORY HAROUTUNIAN*
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829
aberry@justice4you.com
gharoutunian@justice4you.com

Attorneys for Plaintiffs and the Class

** Pro Hac Vice Application Forthcoming*

27528